

FortiGate 日志和消息参考指南

FortiGate 用户手册 第五卷

版本 2.50 MR2
2003 年 8 月 8 日

FortiGate 日志配置和参考指南
版本 2.50 MR2
2003 年八月 8 日

服从规范
FCC Class A Part 15 CSA/CUS

请访问 http://www.fortinet.com 以获取技术支持。

请将在本文档或任何 Fortinet 技术文档中发现的错误信息或疏漏之处发送到 techdoc@fortinet.com。

目录



介绍

本指南描述了如何配置 FortiGate 设备记录网络活动，包括从路由配置的改变到通讯会话以及紧急事件。本指南还逐一解释了日志消息，并对您应当如何处理这些消息提出了建议。

本指南提供了基于 Web 的管理程序和 CLI 操作的步骤说明。

您可以配置 FortiGate 设备去记录六种类型的日志：

- 通讯日志记录所有到达和通过 FortiGate 接口的通讯。您可以将日志配置为记录防火墙策略控制的通讯和任意源地址和目的地址之间的通讯。您还可以使用全局设置，例如会话或者数据包日志。
- 事件日志记录管理和活动事件，例如当某项配置的内容被改变或者添加了一条路由网关的时候记录事件日志消息。
- 病毒日志记录在网页、FTP 和邮件通讯中感染的病毒，例如当 FortiGate 设备检测到一个被感染的文件、阻塞某个类型的文件、阻塞大小超过限制的文件或电子邮件、或者传输一个邮件片段的时候记录病毒日志消息。
- 网页过滤日志记录 HTTP 内容和 URL 阻塞事件，还有例外的 URL 事件。
- IDS 日志记录 FortiGate NIDS 截获的和预防的攻击。
- 电子邮件过滤日志记录在 IMAP 和 POP3 通讯中阻塞的地址模板和内容。

您可以将 FortiGate 设备配置为对下列事件发送报警邮件：

- 病毒事件 （同时记录到事件日志），
- 入侵 （同时记录到 IDS 日志），
- 紧急防火墙或 VPN 事件，或异常 （同时记录到事件日志）。

本指南叙述了如下内容：

文档约定

本指南使用以下约定来描述 CLI 命令的语法。

- 尖括号 <> 所围的内容为可替换的关键词

  例如：

要执行 `restore config <文件名_字符串>`

您应当输入 `restore config myfile.bak`

`<xxx_字符串>` 表示一个 ASCII 字符串关键词。

`<xxx_整数>` 表示一个整数关键词。

`<xxx_ip>` 表示一个 IP 地址关键词。

- 竖线和波形括号 {|} 表示从波形括号中的内容中任选其一。

  例如：

  `set system opmode {nat | transparent}`

  您可以输入 `set system opmode nat` 或 `set system opmode transparent`

- 方括号 [ ] 表示这个关键词是可选的

  例如：

  `get firewall ipmacbinding [dhcpipmac]`

  您可以输入 `get firewall ipmacbinding` 或 `get firewall ipmacbinding dhcpipmac`

Fortinet 的文档

从 FortiGate 用户手册的以下各卷中可以找到关于 FortiGate 产品的对应信息：

- *第一卷：FortiGate 安装和配置指南*

  描述了 FortiGate 设备的安装和基本配置方法。还描述了如何使用 FortiGate 的防火墙策略去控制通过 FortiGate 设备的网络通讯，以及如何使用防火墙策略在通过 FortiGate 设备的网络通讯中对 HTTP、FTP 和电子邮件等内容应用防病毒保护、网页内容过滤和电子邮件过滤。

- *第二卷：FortiGate 虚拟专用网络 （VPN）指南*

  包含了在 FortiGate IPSec VPN 中使用认证、预置密钥和手工密钥加密的更加详细的信息。还包括了 Fortinet 远程 VPN 客户端配置的基本信息，FortiGate PPTP 和 L2TP VPN 配置的详细信息，以及 VPN 配置的例子。

- *第三卷：FortiGate 内容保护指南*

  描述了如何配置防病毒保护，网页内容过滤和电子邮件过滤，以保护通过 FortiGate 的内容。

- *第四卷：FortiGate NIDS 指南*

  描述了如何配置 FortiGate NIDS，以检测来自网络的攻击，并保护 FortiGate 不受其威胁。

- *第五卷：FortiGate 日志和消息参考指南*

  描述了如何配置 FortiGate 的日志和报警邮件。还包括了 FortiGate 日志消息的说明。

- *第六卷：FortiGate CLI 参考指南*

  描述了 FortiGate CLI，并且还包含了一个 FortiGate CLI 命令的说明。

FortiGate 在线帮助也包含了使用 FortiGate 基于 Web 的管理程序配置和管理您的 FortiGate 设备的操作步骤说明。

Fortinet 技术文档的注释

如果您在本文档或任何 Fortinet 技术文档中发现了错误或疏漏之处，欢迎您将有关信息发送到 techdoc@fortinet.com。

客户服务和技术支持

请访问我们的技术支持网站，以获取防病毒保护和网络攻击定义更新、固件更新、产品文档更新，技术支持信息，以及其他资源。网址：http://support.fortinet.com。

您也可以到 http://support.fortinet.com 注册您的 FortiGate 防病毒防火墙或在任何时间登陆到该网站更改您的注册信息。

以下电子邮件信箱用于 Fortinet 电子邮件支持：

amer_support@fortinet.com	为美国、加拿大、墨西哥、拉丁美洲和南美地区的客户提供服务。
apac_support@fortinet.com	为日本、韩国、中国、中国香港、新加坡、马来西亚、以及其他所有亚洲国家和澳大利亚地区的客户提供服务。
eu_support@fortinet.com	为英国、斯堪的纳维亚半岛、欧洲大陆、非洲和中东地区的客户提供服务。

关于 Fortinet 电话支持的信息，请访问 http://support.fortinet.com。

当您需要我们的技术支持的时候，请您提供以下信息：

- 您的姓名
- 公司名称
- 位置
- 电子邮件地址
- 电话号码
- FortiGate 设备生产序列号
- FortiGate 型号
- FortiGate FortiOS 固件版本
- 您所遇到的问题的详细说明



配置日志

日志记录的配置包括选择一个或多个日志记录保存到的位置和选择要记录的日志类型。如果 FortiGate 设备配备了硬盘，您还可以查看、搜索和维护保存到硬盘上的日志。

本章叙述了如下内容：

一般配置步骤

1 将 FortiGate 设备配置为在以下位置记录一个或多个日志：
  • 一台运行系统日志服务的计算机，
  • 一台运行 WebTrends 防火墙报告服务的计算机，
  • FortiGate 硬盘（如果您的 FortiGate 设备配备了一个硬盘的话），
  • FortiGate 系统内存，
  • FortiGate 控制台（仅限于 CLI）。
2 对于每个记录日志的位置，选择日志严重程度的等级。
  FortiGate 将除了低于您所选择的等级之外的所有等级的消息记录到日志。
3 对于记录到本地硬盘的日志，配置最大文件尺寸和其他日志选项。请见 第 6 页 “记录日志”。
4 在每种记录方法的日志策略中，选择 FortiGate 设备记录的日志类型和活动。请见 第 11 页 “配置日志策略”。
5 配置通讯过滤。请见 第 13 页 “配置通讯过滤”。
6 启用某个策略或者接口的通讯日志。请见 第 6 页 “启用通讯日志”。
7 查看、搜索和维护保存在内存或者可选的硬盘中的日志。请见 第 16 页 “查看保存在内存中的日志”和 第 17 页 “查看和维护保存在硬盘上的日志”。



注意：您可以配置 FortiGate 以发送病毒感染事件、入侵、防火墙或 VPN 事件或异常的报警邮件。如果您已经配置 FortiGate 设备将日志消息记录到一个内置的硬盘中，您可以启用在硬盘将满时发送报警邮件的功能。请见 第 21 页 “添加报警邮件地址” 。

启用通讯日志

您可以对通过 FortiGate 接口的通讯记录日志。您还可以对防火墙策略控制的通讯记录日志。

要启用通讯日志，您必须在配置日志策略时（请见 第 11 页 “配置日志策略” ）选择通讯日志，然后执行如下操作：

按照如下操作记录通过一个 FortiGate 接口的通讯的日志

1 进入**系统 > 网络 > 接口。**
2 对于您要启用日志记录的接口，单击它旁边的修改列的编辑。
3 对于日志，单击启用。
4 单击确定。
5 对于每一个您要启用日志记录的接口重复以上操作。

使用 CLI：

```
set system interface <接口名_字符串> config log enable
```

按照如下对防火墙策略控制的通讯记录日志

1 进入 **防火墙 > 策略。**
2 单击一个策略标签。
3 单击通讯日志。
4 单击确定。

使用 CLI：

```
set firewall policy srcintf <源接口_字符串> dstintf <目的接口_字符串> policyid <策略编号_整数> logtraffic enable
```

记录日志

您可以配置日志记录功能将日志记录到以下一个或多个地点：

- 一台运行系统日志服务的计算机，
- 一台运行 WebTrends 防火墙报告服务的计算机，
- FortiGate 硬盘 (如果您的 FortiGate 设备配备了一个硬盘的话)，
- FortiGate 控制台 (仅限于 CLI)。

如果您的 fortiGate 设备没有装备硬盘，您也可以将日志记录配置为将事件日志和攻击日志记录到 FortiGate 系统内存，以允许对最近的日志条目的快速访问。如果 FortiGate 设备重新启动，所有的日志条目都将丢失。



注意：不是所有型号的 FortiGate 设备都有可选装的硬盘，FortiGate-50 没有将日志记录到内存的功能。

您可以对每个日志位置选择相同或者不同的严重程度级别。例如，您可能希望只将紧急和警报级的消息记录到 FortiGate 内存，而将全部级别的消息记录到一台远程主机。请见 第 25 页 “ 日志消息严重程度” 。

关于过滤 FortiGate 设备记录的日志类型和动作的详细信息，请见 第 11 页 “ 配置日志策略” 和 第 13 页 “ 配置通讯过滤” 。

本节叙述了如下内容：

- 在远程计算机上记录日志
- 在 NetIQ WebTrends 服务器上记录日志
- 将日志记录到 FortiGate 硬盘
- 将日志记录到系统内存
- 将日志记录到控制台

在远程计算机上记录日志

以下操作用于将 FortiGate 配置为将日志消息记录到一台远程电脑上。这台远程电脑必须配置为一个系统日志服务器。

1 进入 **日志与报告 > 日志设置**。

2 选择 **记录日志到远程主机** 以发送日志到一个日志服务器上。

3 输入运行系统日志服务器软件的远程主机的 IP **地址** 。

4 输入系统日志服务器的端口号。

5 选择您要记录的日志消息的严重程度级别。

FortiGate 将记录下除了低于您选择的级别的全部级别的日志。例如，如果您希望记录紧急、警报、危险和错误级的消息，选择错误级。

6 选择配置策略。

- 选择您希望 FortiGate 设备记录日志的日志类型。
- 对于每一种类型的日志，选择您希望 FortiGate 设备记录日志消息的行为。
- 单击确定。

关于日志类型和行为的详细信息，请见 第 11 页 “ 配置日志策略” 和 第 13 页 “ 配置通讯过滤” 。

7 单击应用。

使用 CLI：

```
set log setting syslog loglevel <严重级别_整数> server <系统日志服务器_ip> status enable

set log policy destination syslog traffic status enable
```

```
set log policy destination syslog event status enable
category {configuration | ipsec | dhcp | ppp | login | ipmac |
system | ha | auth | routegateway | none}

set log policy destination syslog virus status enable
category {detectvirus | signatureupdate | none}

set log policy destination syslog webfilter status enable
category {bannedword | script | url | none}

set log policy destination syslog ids status enable category
{detection | prevention | none}
```

在 NetIQ WebTrends 服务器上记录日志

以下操作可以将 FortiGate 配置为在一台远程的 NetIQ 防火墙报告服务器上记录日志，以供存储和分析之用。FortiGate 日志的格式服从 Web Trends Enhanced Log（WELF）格式规范，并与 Web Trends NetIQ 安全报告中心 2.0 和防火墙套件 4.1 兼容。可以从安全报告中心和防火墙套件的文档中获得更详细的信息。



注意：FortiGate 通讯日志消息包括发送和接收域，这些项是可选的，但是对于绘制 WebTrends 图是必须的。

以下操作将日志记录到一台 NetIQ Web Trends 服务器上。

1. 进入 **日志与报告 > 日志设置**。
2. 选择 以 Web Trends Enhanced 日志格式记录日志。
3. 输入 NetIP WebTrends 防火墙报告服务器的 **IP 地址**。
4. 选择您要记录的日志消息的严重程度级别。
   FortiGate 将记录下除了低于您选择的级别的全部级别的日志。例如，如果您希望记录紧急、警报、危险和错误级的消息，选择错误级。
5. 选择配置策略。
   要配置 FortiGate 设备过滤记录的日志类型和事件，按照 第 11 页 “ 配置日志策略” 和 第 13 页 “ 配置通讯过滤” 中的步骤操作。
6. 单击应用。

使用 CLI：

```
set log setting webtrends status enable server <服务器_ip>
loglevel <严重级别_整数>
```

将日志记录到 FortiGate 硬盘

如果您的系统中安装了硬盘，您可以将日志文件记录到硬盘里。

以下操作设置日志的记录方式为记录到硬盘：

1. 进入**日志与报告 > 日志设置**。
2. 选择 **记录到本地** 。
3. 输入一个日志文件的最大值 （以兆字节为单位）。
   当日志文件的大小达到这一最大值的时候，当前日志文件将被关闭并保存。系统将创建一个新的当前日志文件用来记录日志。默认的最大系统日志文件的大小是 10M 字节，最大系统日志文件的大小是 2G 字节。

4 输入一个创建日志的 时间间隔 （以天为单位）。

在达到指定的时间间隔后，当前日志文件将被关闭并保存，一个新的文件被创建。默认的时间间隔是 10 天。

5 选择您要记录的日志消息的严重程度级别。

FortiGate 将记录下除了低于您选择的级别的全部级别的日志。例如，如果您希望记录紧急、警报、危险和错误消息，选择错误级。

6 选择配置策略。

要配置 FortiGate 设备过滤记录的日志类型和事件，按照 第 11 页 “ 配置日志策略” 和 第 13 页 “ 配置通讯过滤” 中的步骤操作。

7 设置当磁盘被写满时的日志选项：

覆盖	当硬盘满的时候删除最早的日志文件。覆盖是默认的选项。
阻塞数据流	当硬盘被写满的时候阻塞所有的网络流通。
不记录日志	当硬盘被写满的时候停止记录日志消息。

8 单击 **应用** 保存您的日志设置。

图 1: 带有可选硬盘的日志设置举例



使用 CLI：

```
   set log setting local status enable
set log setting local loglevel <严重级别_整数>
   set log setting local filesz <文件大小_整数>
   set log setting local logtime <日志有效期_整数>
   set log setting local diskfull
{overwrite | blocktraffic | nolog}
```

将日志记录到系统内存

如果您的 FortiGate 没有安装硬盘，您可以使用以下操作将 FortiGate 配置为保留一些系统内存用来记录当前的日志消息。将日志记录到内存使得您可以快速地访问最近的日志条目。FortiGate 可以在系统内存中保留有限的日志消息。一旦所有的可用内存都被用掉了，FortiGate 会删除最早的日志消息。如果 FortiGate 重新启动，所有的记录都会丢失。



注意：FortiGate-50 没有将日志记录到内存的功能。



注意：FortiGate 只能在系统内存中记录事件日志和攻击日志。

以下操作可以将日志记录到内存：

1 进入 **日志与报告 > 日志设置**。

2 选择 **在内存中记录日志**。

3 选择您要记录的日志消息的严重程度级别。

FortiGate 将记录下除了低于您选择的级别的全部级别的日志。例如，如果您希望记录紧急、警报、危险和错误消息，选择错误级。

4 选择配置策略。

要配置 FortiGate 过滤记录的日志的类型和事件，按照 第 11 页 “ 配置日志策略” 中的步骤操作。

5 单击应用。

图 2: 没有可选硬盘的日志设置举例



使用 CLI：

```
set log setting memory status enable
set log setting memory loglevel <严重程度_整数>
```

```
set log policy destination memory
{traffic | event | virus | webfilter | ids | emailfilter | update} status enable
```

将日志记录到控制台

您可以使用 CLI 将 FortiGate 配置为将日志消息发送到控制台，以便立即查看。将日志记录到控制台允许对最近的日志条目的快速访问。

使用 CLI：

```
set log policy destination console
{traffic | event | virus | webfilter | ids | emailfilter | update} status enable
set log setting console status enable
```

配置日志策略

您可以配置哪些日志需要被记录和在每一种日志中记录那些类别的日志。

1 进入**日志和报告 > 日志设置**。

2 对于您在 第 6 页 “ 记录日志” 中选择的每一种日志位置选择配置策略。

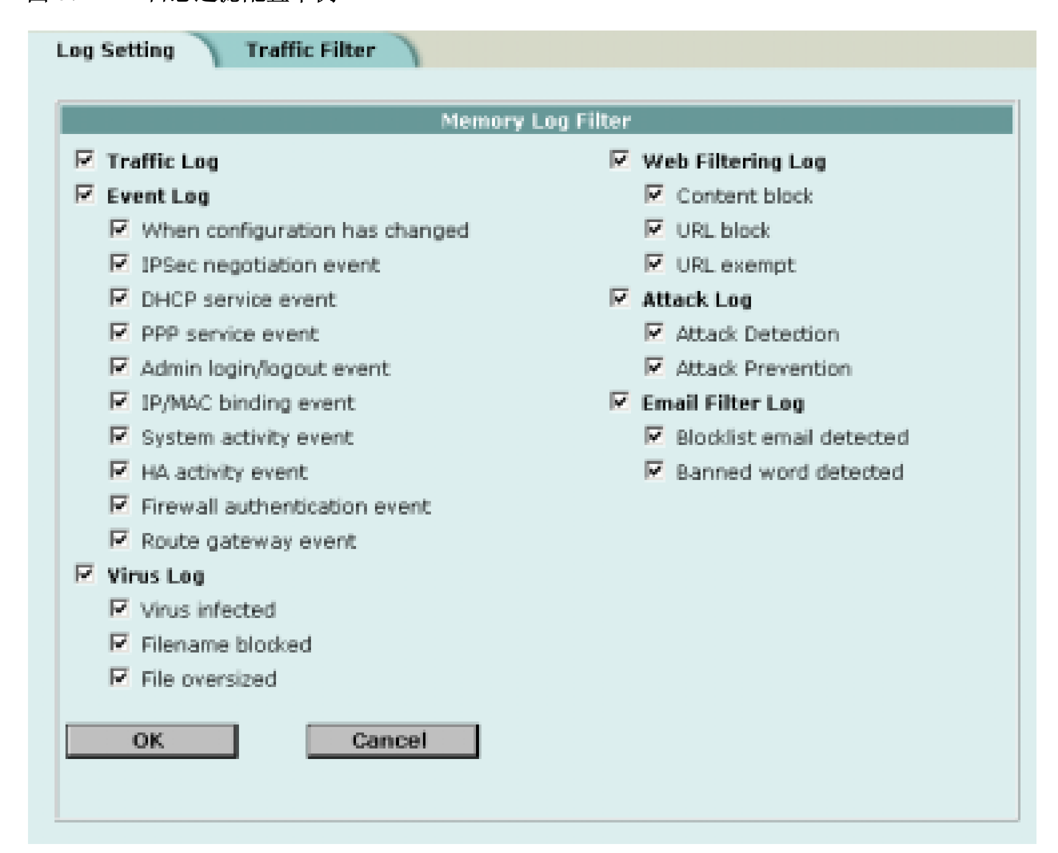
3 选择您希望 FortiGate 设备记录的日志类型。

通讯日志	记录到此接口或者通过此接口的全部连接，或者防火墙策略接受的连接。要配置通讯过滤，请见 第 13 页 “ 配置通讯过滤” 。
事件日志	在事件日志中记录管理和活动事件。 管理事件包括系统配置的变动和管理员、用户的登录和登出。动作事件包括系统活动，例如建立 VPN 通道和 HA 失效恢复事件。
病毒日志	记录病毒入侵事件，例如当 FortiGate 设备检测到一个病毒、阻塞一个类型的文件或者阻塞一个超大的文件或邮件时生成此日志消息。
网页过滤日志	记录活动事件，例如 URL 和内容阻塞，以及从阻塞中排除 URL。
IDS 日志	记录 NIDS 检测到的攻击和 NIDS 预防模块预防的攻击。
邮件过滤日志	记录活动事件，例如检测到包含有不受欢迎的内容的邮件和来自不受欢迎的发件人的邮件。

4 如果您在步骤 3 中选择了事件日志、病毒日志、网页过滤日志或者 IDS 日志，您可以选择希望 FortiGate 设备记录的日志分类。

5 单击确定。

图 3: 日志过滤配置举例



使用 CLI：

```
   set log policy destination
{syslog | webtrends | local | console} traffic status enable

   set log policy destination
{syslog | webtrends | local | console} event status enable
category {configuration | ipsec | dhcp | ppp | login | ipmac |
system | ha | auth | routegateway | none}

   set log policy destination
{syslog | webtrends | local | console} virus status enable
category {detectvirus | signatureupdate | none}

   set log policy destination
{syslog | webtrends | local | console} webfilter status enable
category {bannedword | script | url | none}

   set log policy destination
{syslog | webtrends | local | console} ids status enable
category {detection | prevention | none}

   set log policy destination
{syslog | webtrends | local | console} emailfilter status
enable category {email | bword | none}
```

配置通讯过滤

FortiGate 设备可以根据任何源地址、目的地址和服务过滤通讯。您也可以启用以下全局设置：

- 将 IP 地址解析为主机名，
- 记录会话和数据包信息，
- 显示端口号或服务。

通讯过滤列表显示被过滤的通讯的名称、源地址和目的地址，以及通讯类型。



注意：如果您选择了某个防火墙策略的记录通讯日志功能，也记录通讯日志。请见 *防火墙策略指南* 中的 “添加 NAT/ 路由模式策略” 和 “添加透明模式策略”。



注意：FortiGate 设备只能在系统内存中记录事件日志和攻击日志。

本节叙述了如下内容：

配置通讯过滤设置

按照如下步骤配置在全部通讯日志消息中记录的信息。

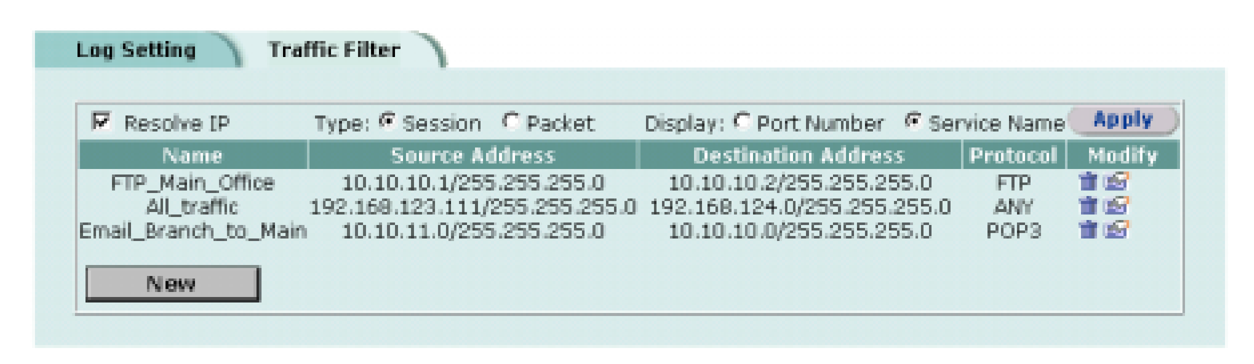
1 进入 **日志和报告 > 日志设置 > 通讯过滤。**

2 选择您要应用到全部通讯日志消息的设置。

解析 IP	如果您希望通讯日志消息列出 IP 地址和存储在 DNS 服务器中的域名，选择解析 IP。如果您还没有添加由您的 ISP 提供的主 DNS 服务器和辅助 DNS 服务器地址，进入 **系统 > 网络 >DNS** 并添加地址。
类型	选择会话和数据包。如果您选择了会话，FortiGate 设备记录每个会话发送和接收的数据包的数量。如果您选择了数据包，FortiGate 设备记录每个会话的数据包长度的平均值 （以字节为单位）。
显示	如果您希望通讯日志消息中列出端口号，则选择端口号。例如，80/TCP。如果您希望通讯日志消息列出服务的名称，则选择服务名，例如，TCP。

3 单击应用。

图 4: 通讯过滤列表举例



使用 CLI：

```
set log trafficfilter setting resolve {enable | disable}
type {session | packet} display {port | name}
```

添加通讯过滤条目

按照如下步骤在通讯过滤列表中添加条目。

1 进入**日志和报告 > 日志设置 > 通讯过滤**。

2 单击新建。

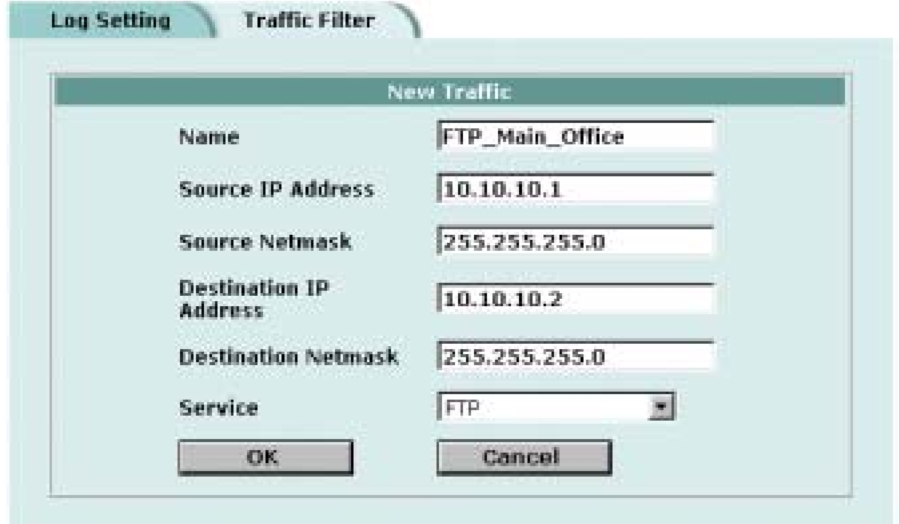
3 输入您希望 FortiGate 设备记录通讯日志消息的通讯的信息。

名称	输入一个名称以识别这个通讯。 这个名称可以包含数字 （0-9），大写和小写字母 （A-Z, a-z），以及特殊字符 - 和 _。不能使用其他特殊字符和空格。
源 IP 地址 **源网络掩码**	输入你希望 FortiGate 设备记录通讯日志消息的源 IP 地址和网络掩码。地址可以是单独的计算机、子网或者整个网络。
目的 IP 地址 **目的掩码**	输入您希望 FortiGate 设备记录通讯日志消息的目的 IP 地址和掩码。这个地址可以是单独的计算机，子网或者网络。
服务	为您希望 FortiGate 设备记录的通讯日志消息选择服务组或者单独的服务。

4 单击确定。

通讯过滤列表将显示新的通讯地址条目 The traffic filter list，以及您在 第 13 页 “ 配置通讯过滤设置” 选择的设置。

图 5: 新的通讯地址条目举例



使用 CLI：

set log trafficfilter rule <名称> src <源_ip> <网络掩码_ip> dst <目的_ip> <网络掩码_ip> service <服务_字符串>

编辑通讯过滤条目

按照如下步骤编辑通讯过滤列表中的条目。

1 进入**日志和报告 > 日志设置 > 通讯过滤**。
2 对于您要编辑的通讯条目，单击它旁边的修改列的编辑。
3 编辑名称、地址和服务信息。
4 单击确定。

使用 CLI：

set log trafficfilter rule <名称_字符串> src <源_ip> <掩码_ip> dst <目的_ip> <掩码_ip> service <服务_字符串>

删除通讯过滤条目

按照如下步骤删除通讯过滤列表中的条目。

1 进入**日志和报告 > 日志设置 > 通讯过滤**。
2 对于您要删除的通讯条目，单击它旁边的修改列的删除 。
3 单击确定。

输入 CLI：

unset log filter traffic rule <名称_字符串>

查看保存在内存中的日志

如果 FortiGate 被配置为在内存中记录日志。您可以使用基于 Web 的管理程序来查看、搜索和清除日志中的消息。

本节讨论了：



注意：FortiGate-50 没有将日志记录到内存的功能。

查看日志

在日志消息列表中，消息按照时间顺序排列，生成时间晚的消息排在上面。以下操作用于查看保存在系统内存中的日志：

1 进入**日志与报告 > 记录日志**。

2 选择 **事件日志** 、**攻击日志**、**病毒防护日志**、**网页过滤日志**或者**电子邮件过滤日志**。
基于 Web 的管理程序列出了保存在系统内存中的日志消息。

3 滚动窗口可以查看到更多的日志消息。

4 要查看日志中的某一行，只需在转到某行的空白处填写行号，然后单击 Go。

5 要在日志消息中翻页，单击 **向下翻页** 或 **向上翻页** 。



注意：在 第 23 页 “ 日志格式” 和每种类型的日志的章节中有关于日志消息格式的说明。

使用 CLI：

```
get log elog
```

搜索日志

使用以下操作可以搜索保存在系统内存里的日志消息。

1 进入 **日志与报告 > 记录日志**。

2 选择 **事件日志** 、**攻击日志**、**病毒防护日志**、**网页过滤日志**或者**电子邮件过滤日志**。

3 单击 可以在选定的日志中搜索消息。

4 选择 **与** 可以搜索与所有给定条件匹配的消息。

5 选择 **或** 可以搜索与某个或多个给定条件匹配的消息。

6 选择以下一个或多个搜索条件：

关键词	可以搜索包含在消息中的任何文字。关键词搜索中区分大小写字母。
时间	搜索日志中创建时间符合给定的年、月、日、小时条件的日志。

7 单击 **确定** 开始搜索
基于 Web 的管理程序会显示出符合给定搜索条件的日志消息。您可以卷动窗口查看消息或者进行另一次搜索。



注意：在进行了一次搜索之后，如果想再次显示所有的日志消息，只需清空所有的搜索条件并再次执行搜索。

清除日志消息

按以下步骤清除日志：

1 进入 **日志与报告 > 记录日志**。
2 选择 **事件日志** 、**攻击日志**、**病毒防护日志**、**网页过滤日志**或者**电子邮件过滤日志**。
3 单击 清除选定日志中的所有消息。
4 单击 **确定**。

查看和维护保存在硬盘上的日志

如果您的 FortiGate 的日志是记录在硬盘上的，您可以用以下方法查看、搜索和维护流量日志、事件日志和攻击日志：

- 查看日志
- 搜索日志
- 将日志文件下载到管理员电脑
- 删除当前日志中的所有消息
- 删除一个保存了的日志文件

查看日志

在日志消息列表中，最近生成的消息被排在最上面。您可以用以下操作查看活动的或者保存了的流量日志、事件日志或者攻击日志：

1 进入**日志与报告 > 记录日志**。
2 选择 **事件日志** 、**攻击日志**、**病毒防护日志**、**网页过滤日志**或者**电子邮件过滤日志**。
基于 Web 的管理程序列出了选定类型的日志中所有保存了的消息。 当前日志文件在列表的顶端。列表显示了每个日志中最后一条信息写入日期和时间、日志文件的大小和日志名。
3 对要查看的日志文件，单击 **查看** 。
4 基于 Web 的管理程序中显示出选定的日志中的消息。
5 您可以设定每页可以显示的日志的消息数目，可选的设定值为 30、50 或 1000。您可以通过卷动窗口查看其它的消息。
6 要查看日志文件中的指定行，只需在转到行字段填写要查看的行号。然后单击 。
7 要在日志消息中翻页，单击 **向下翻页** 或 **向上翻页** 。
8 要在您所查看的日志中搜索某条消息，单击**搜索** 。



注意：在 第 23 页 “ 日志格式” 和每种类型的日志的章节中有关于消息格式的说明。

使用 CLI：

```
get log elog
```

搜索日志

以下操作用于在被保存的日志或当前日志中搜索消息：

1. 进入 **日志与报告 > 记录日志**。
2. 选择 **事件日志** 、**攻击日志**、**病毒防护日志**、**网页过滤日志**或者**电子邮件过滤日志**。
3. 对要查看的日志文件，单击查看 。
4. 单击 在您正在查看的日志文件中搜索消息。
5. 选择 **与** 可以搜索与所有给定条件都匹配的消息。
6. 选择 **或** 可以搜索与某个或多个给定条件匹配的消息。
7. 选择以下一个或多个搜索条件：

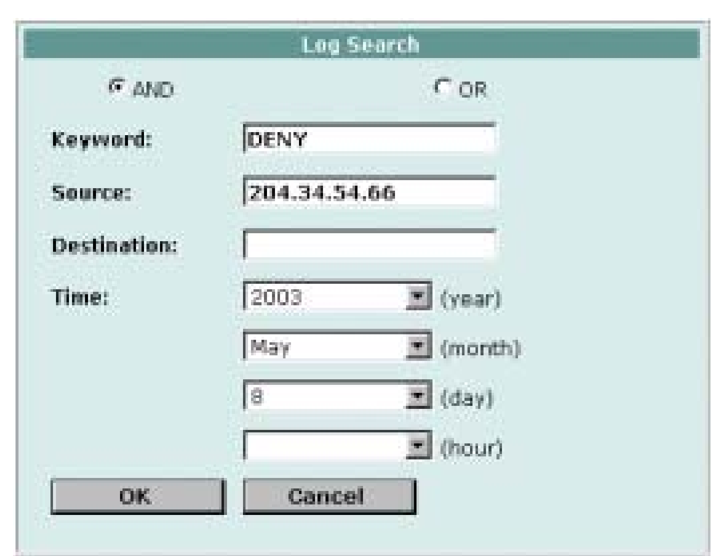
关键词	可以搜索包含在消息中的任何文字。关键词搜索中区分大小写字母。
源地址	按照指定的源 IP 地址搜索 （仅限于流量日志和攻击日志）。
目的地址	按照指定的目的 IP 地址搜索 （仅限于流量日志和攻击日志）。
时间	搜索日志中创建时间符合给定的年、月、日、小时条件的日志。

8. 单击 **确定** 开始搜索。
基于 Web 的管理程序会显示出符合给定搜索条件的日志消息。您可以卷动窗口查看消息或者进行另一次搜索。



注意：在进行了一次搜索之后，如果想再次显示所有的日志消息，只需清空所有的搜索条件并再次执行搜索。

图 6: **搜索通讯日志的例子**



将日志文件下载到管理员电脑

您可以将日志文件下载到管理员电脑上保存为纯文本文件。下载完日志之后，可以用任何文本编辑器查看日志文件。以下操作用于下载日志文件：

1. 进入 **日志与报告 > 记录日志**。
2. 选择 **事件日志** 、**攻击日志**、**病毒防护日志**、**网页过滤日志**或者**电子邮件过滤日志**。
   基于 Web 的管理程序列出了选定类型的日志中所有保存了的消息。当前日志文件在列表的顶端。列表显示了每个日志中最后一条信息写入日期和时间、日志文件的大小和日志名。
3. 对要下载到管理员电脑上的日志文件，单击 。
4. 单击 **保存** 将日志文件下载到管理员电脑上并保存为文本文件。

删除当前日志中的所有消息

以下操作用于从活动的日志中删除所有消息：

1. 进入 **日志与报告 > 记录日志**。
2. 选择 **事件日志** 、**攻击日志**、**病毒防护日志**、**网页过滤日志**或者**电子邮件过滤日志**。
   基于 Web 的管理程序列出了选定类型的日志中所有保存的消息。当前日志文件在列表的顶端。列表显示了每个日志中最后一条信息写入日期和时间、日志文件的大小和日志名。
3. 单击 **清空** 以删除选定的当前日志中的所有消息。
4. 单击 **确定** 以删除消息。

删除一个保存了的日志文件

以下步骤用于删除一个保存了的日志文件：

1. 进入**日志与报告 > 记录日志**。
2. 选择 **事件日志** 、**攻击日志**、**病毒防护日志**、**网页过滤日志**或者**电子邮件过滤日志**。
   基于 Web 的管理程序列出了选定类型的日志中所有保存了的消息。当前日志文件在列表的顶端。列表显示了每个日志中最后一条信息写入日期和时间、日志文件的大小和日志名。
3. 对于要删除的日志文件，单击 以删除这个日志文件。
4. 单击 **确定** 以删除日志文件。



发送报警邮件

您可以将 FortiGate 设备配置为当有病毒事件、阻塞事件、网络入侵或者其他防火墙、VPN 事件和异常的时候向最多三个地址发送警报邮件。当您设置完邮件地址之后，可以通过发送测试邮件测试您的设置。

本节叙述了如下内容：

添加报警邮件地址

因为 FortiGate 设备使用 SMTP 服务器名连接邮件服务器，所以它需要在您的 DNS 服务器上搜索这个名称。因此，在您配置报警邮件之前，您至少要先配置一个 DNS 服务器。

按照如下方法添加 DNS 服务器。

1 进入**系统 > 网络 >DNS**。

2 如果还没有添加 DNS 服务器，添加您的 ISP 提供的主 DNS 服务器和辅助 DNS 服务器地址。

3 单击应用。

添加报警邮件地址

1 进入 **日志和报告 > 报警邮件 > 配置**。

2 如果您所使用的 SMTP 服务器要求用户名和密码进行登录，在认证选项单击启用。

3 在 SMTP 服务器域，输入 FortiGate 设备用来发送邮件的 SMTP 服务器的名称。按照如下格式输入：`smtp.domain.com`。
SMTP 服务器可以位于任何连接到 FortiGate 设备的网络中。

4 在 SMTP 用户栏，按照如下格式输入一个有效的邮件地址：`user@domain.com`。
这个地址将出现在报警邮件的表头。

5 在密码栏，输入这个 SMTP 用户用来访问 SMTP 服务器的密码。

6 在邮件发送到栏，最多可以输入三个邮件目的地址。
这些地址是 FortiGate 设备将报警邮件实际发送到的地址。

7 单击应用。

使用 CLI：

```
set system dns primary <服务器_ip>
set system dns secondary <服务器_ip>
set alertemail configuration server <smtp服务器_ip> user
<smtp用户名_字符串> passwd <密码_字符串> mailto <电子邮件地址1_字符串>
<电子邮件地址2_字符串> <电子邮件地址3_字符串>
```



注意：您可以使用 CLI 为 SMTP 用户指定一个密码。

测试报警邮件

您可以通过发送测试邮件的方法测试报警邮件设置是否正确：

1 进入 **日志与报告 > 报警邮件 > 配置**。
2 单击 **测试** ，从 FortiGate 发送测试邮件到您所配置的邮件地址。

启用报警邮件

您可以配置 FortiGate 发送报警邮件来响应以下事件：病毒事件、入侵企图、以及防火墙或者 VPN 事件。如果您已经配置了将日志存储到本地硬盘，则可以启用当硬盘快被写满时发送报警邮件的功能。按照以下步骤启用报警邮件：

1 进入 **日志与报告 > 报警邮件 > 分类**。
2 选择 **启用病毒事件的报警邮件** 可以使 FortiGate 在防病毒扫描功能发现病毒时发送报警邮件。

   当病毒文件阻塞功能删除一个文件时不会发送此邮件。

3 选择**启用阻塞事件报警邮件**可以使 FortiGate 设备在阻塞被病毒感染的文件时发送一封报警邮件。
4 选择**启用入侵事件的报警邮件**可以使 FortiGate 发送报警邮件通知系统管理员 NIDS 检测到了攻击活动。
5 选择 **启用防火墙 /VPN 紧急事件或者异常的报警邮件** 可以使 FortiGate 在出现防火墙或 VPN 的紧急事件时发送报警邮件。

   防火墙关键事件包括失败了的认证企图。
   VPN 关键事件包括重放检测功能检测到一个重放的数据包。重放检测功能可以配置在自动密钥 VPN 通道或者手工密钥 VPN 通道里。

6 选择 **在硬盘满时发送报警邮件** 可以使 FortiGate 在硬盘快被写满时发送报警邮件。
7 单击 **应用** 。

使用 CLI：

```
set alertemail setting option {virusincidents intrusions
critical diskfull | none}
```

日志格式

FortiGate 日志消息可以分成两部分：

- 日志报头
- 日志正文

在下面的事件日志的例子中，报头部分将使用粗体标记。

2003-05-23 16:23:46 log_id=0100030101 type=event subtype=config pri=information user=admin ui=GUI(192.168.100.98) module=user submodule=local msg="Local user user1 has been added by user admin via GUI(192.168.100.98)"

日志报头

日志报头部分可以包含以下信息：

年年年年 - 月月 - 日日 时时 : 分分 : 秒秒 日志 _id 设备 _id 分类 - 子类 - 严重程度

日期	显示事件发生的年、月、日。
时间	显示事件发生的时、分、秒。
日志 ID	十进制数字编号。头两位是分类号，后边的两位是子类号。请见 第 24 页 “ 日志分类和子类” 。最后 6 位根据具体的情况而不同。
设备 ID	FortiGate 设备的序列号。
分类	分类名是系统中事件所属的部分。分类可以是通讯、事件、病毒、网页过滤、NIDS 或者邮件过滤。请见 第 24 页 “ 日志分类和子类” 。
子类	子类名是消息的类型。请见 第 24 页 “ 日志分类和子类” 。
严重程度	严重程度将事件分为 8 个级别，从紧急到调试。请见 第 25 页 “ 日志消息严重程度” 。

日志分类和子类

FortiGate 日志消息使用以下分类和子类：

表 1：日志消息分类和子类

分类编号	分类	子类编号	子类
1	通讯	00	数据包——数据包日志
		01	会话——会话日志
2	事件	00	配置——当配置被修改时记录
		01	ipsec——IPSec 协商事件
		02	dhcp --DHCP 服务事件
		03	ppp——PPP 服务事件
		04	login——管理员登录 / 登出事件
		05	ipmac -- IP/MAC 绑定事件
		06	系统——系统活动事件
		07	HA——HA 活动事件
		08	认证——防火墙认证事件
		09	路由网关——路由网关事件
3	病毒	00	感染——病毒感染
		01	文件名——文件名被阻塞
		02	超大——文件超过规定大小
4	网页过滤	00	内容——内容阻塞
		01	URL 阻塞——URL 阻塞
		02	URL 排除——从阻塞中排除 URL
5	IDS	00	检测——IDS 检测
		01	预防——IDS 预防
6	电子邮件过滤	00	电子邮件——检测到的阻塞邮件列表
		01	禁忌词汇——检测到的禁忌词汇

日志消息严重程度

FortiGate 将日志记录的严重程度分为 8 个级别。在 CLI 中使用级别编号配置严重程度级别。在基于 Web 的管理程序中使用严重程度名称配置严重程度级别。在日志消息中使用级别的缩写。

表 2: 日志消息严重程度级别

级别编号	级别名称	级别缩写	含义
0	紧急	emerg	系统即将无法运行。
1	警报	alert	需要立即采取措施。
2	危机	criti	功能受到影响。
3	错误	error	存在一个错误的事件，并且可能影响到系统的功能。
4	警告	warni	功能可能受到影响。
5	注意	notif	关于一般事件的信息。
6	消息	infor	关于系统操作的常规信息。
7	调试	debug	用于调试操作的详细信息。

根据日志消息发送到的地点的不同，日志报头的格式稍有差别。关于日志地点的详细信息请见 第 6 页 “ 记录日志” 。

本地 / 内存日志报头格式

如果您将日志配置为记录到本地硬盘或者内存，日志报头的格式类似于下面的例子：

```
2003-05-23 16:23:46 log_id=0100030101 type=event
subtype=config pri=information
```

Webtrends 日志报头格式

如果您将日志配置为记录到一个远程 NetIQ WebTrends 防火墙报告中心，日志报头的格式类似于下面的例子：

```
id=firewall time="2003-05-21 14:01:01" fw=FGT4002801021089
pri=6 log_id=0100030101 type=event subtype=configure
```

远程系统日志日志报头格式

如果您将日志配置为记录到一个远程系统日志服务器，日志报头有以下两种格式：

CSV 格式

如果您在配置日志设置的时候启用了 CSV 格式，日志报头格式类似于下面的例子：

```
date=2003-05-21, time=14:01:01, device_id=FGT4002801021089,
pri=information, log_id=0100030101, type=event,
subtype=configure
```

非 CSV 格式

如果您在配置日志设置的时候没有启用 CSV，日志报头的格式将类似于下面的例子：

```
date=2003-05-21 time=14:01:01 device_id=FGT4002801021089
pri=information log_id=0100030101 type=event subtype=configure
```

日志正文

日志正文包括事件或活动的详细信息，例如 IP 地址和动作状态。除了通讯日志之外，其他日志的条目中，在日志正文的末尾还包括例如类似于下面例子中所显示的日志消息：

```
user=admin ui=GUI(192.168.100.98) module=user
submodule=local msg="Local user user1 has been added by user
admin via GUI(192.168.100.98)"
```

事件日志正文

事件日志记录管理和行为事件。管理事件包括对系统配置的修改，管理员和用户的登录和登出。行为事件包括系统活动、例如 VPN 通道的建立和防火墙认证事件。

每个事件日志消息记录了事件发生的日期和事件，以及一个对事件的描述。对于到 FortiGate 设备的以管理为目的的连接和对配置的修改，事件日志消息还包含了管理者电脑的 IP 地址。

一个事件日志正文的例子包含了如下信息：

```
2003-05-12 07:36:00 event-admin-information: user=admin
ui=ssh(10.10.10.1) action=logout status=success reason=timeout
msg="User admin logout from ssh(10.10.10.1),time out"
```

关于事件日志消息的详细信息请见 第 29 页 “ 事件日志消息” 。

病毒日志正文

每个病毒日志消息记录了检测到病毒的日期和时间，病毒的类型，以及被感染的通讯的源 IP 地址和目的 IP 地址。

一个病毒日志正文的例子包含如下信息：

```
src=<IP地址> dst=<IP地址> src_int=<源_接口_名称> dst_int=<目的_接口_名称> service= {http | smtp | pop3 | imap | ftp}
status={blocked | passthrough} from=<发件人电子邮件地址> to=<收件人电子邮件地址> msg="<消息字符串>"
```

关于病毒日志消息的详细信息 请见 第 48 页 “ 病毒日志消息” 。

网页过滤日志正文

每个网页过滤日志消息记录了内容被阻塞、URL 被阻塞或者 URL 被从阻塞中排除的日期和时间，以及 HTTP 通讯的源 IP 地址和目的 IP 地址。

一个网页过滤日志正文的例子包含如下信息：

```
src=<IP地址> dst=<IP地址> src_int=<源_接口_名称> dst_int=<目的_接口_名称> service=http status={blocked | passthrough} dstname=<主机名称> arg=<URL 的路径名> msg="<消息字符串>"
```

关于网页日志消息的详细内容请见 第 48 页 “ 网页过滤日志消息” 。

IDS 日志正文

IDS 日志记录了被 FortiGate NIDS（请见 *FortiGate 网络防护指南* 中的网络入侵检测系统 （NIDS））检测到的攻击。每个 IDS 日志消息记录了攻击发生的日期和时间，攻击的类型以及这次攻击的源 IP 地址和目的 IP 地址。

一个 IDS 日志正文的例子包括如下内容：

```
2003-05-09 08:13:17 ids-detec-alert: attack_id=102891683
src=192.155.122.73 dst=192.155.48.21 src_port=1066 dst_port=80
status=detected proto=006 service=http msg="Web-Misc. whisker
HEAD with large datagram"
```

关于 IDS 日志消息的详细信息请见 第 49 页 “ IDS 日志消息” 。

电子邮件过滤日志正文

每个电子邮件过滤日志消息记录了根据地址模板或者内容阻塞的日期和时间，以及 IMAP 或 POP3 通讯的源 IP 地址和目的 IP 地址。

一个电子邮件过滤日志正文的例子包含如下内容：

src=<IP地址> dst=<IP地址> src_int=<源_接口_名称> dst_int=<目的_接口_名称> service= {http | smtp | pop3 | imap | ftp} status={blocked | passthrough} from=<发件人电子邮件地址> to=<收件人电子邮件地址> msg="<消息字符串>"

通讯日志正文

通讯日志正文记录了到达和通过 FortiGate 接口的全部通讯。关于如何配置通讯日志的详细信息，请见 第 13 页 “ 配置通讯过滤” 。

如果通讯过滤类型被设置为会话，通讯日志包括了接收和发送的数据包的数量。

如果通讯过滤类型被设置为数据包，通讯日志包括了平均数据包大小。

通讯日志正文不包含消息文本。

一个通讯日志正文的例子包含了如下内容：

duration=<持续时间_数字> policyid=<策略ID_数字> proto=<协议_数字> service=<服务_字符串> status=<{拒绝 | 接受}> src=<源_IP地址> srcname=<源名称_字符串> dst=<目的_IP地址> dstname=<目的名称_字符串> src_int=<源接口名称_字符串> dst_int=<目的接口名称_字符串> sent=<发送_数字> rcvd=<接收_数字> send_pkt=<发送数据包_数字> rcd_pkt=<接收数据包_数字> src_port=<源端口号_数字> dst_port=<目的端口号_数字> vpn=<VPN通道名称_字符串> tran_ip<转换IP地址> tran_port=<转换端口号_数字> dir_disp=<源 | 重放> tran_disp=<noop|snat|dnat>

持续时间	以秒为单位的会话或者数据包持续的时间。
策略 ID	这个通讯类型使用的策略。
协议	在 IP 报头中的协议编号。

服务	• 对于 TCP 和 UDP 通讯，服务是 "dst_port_number/tcp" 或者 "dst_port_number/udp"。 • 对于 ICMP，应该是 "icmp"。 • 对于其他通讯，应该是 "unknown"。 如果日志设置或者通讯过滤的显示设置为服务名： • 对于 TCP 通讯，服务将被解析为 "echo", "daytime", "netstat", "qotd", "ftp-data", "ftp", "ssh", "telnet", "smtp", "time", "nameserver", "dns", "gopher", "finger", "http", "hostnames", "pop3", "imap", "imap3", 和 "https"。 • 对于 UDP 通讯，服务将被解析为 "echo", "daytime", "ssh", "time", "dns", "tftp", "gopher", "http", "pop3", "imap", "imap3", "https". • 如果它不能被解析为上面所列出的服务名，则将显示为 "dst_port_number/tcp" 或者 "dst_port_number/udp"。 • 对于其他通讯，将显示为 "other"。
状态	拒绝或接受。
源	通讯发送者的源 IP 地址。
源名	发送者的 IP 地址或者名称。
目的	接收者的 IP 地址。
目的名	接收者的 IP 地址或名称。
源接口	通讯进入的接口，对于从防火墙向外发出的通讯它将是 “未知”。
目的接口	通讯发出的接口，对于进入防火墙的向内的通讯它将是 “未知”。
发送	以字节为单位统计的通讯发送的数据总数。
接收	以字节为单位统计的通讯接收的数据总数。
发送 - 数据包	当前会话中发送的数据包的总数。仅限于会话日志。
接收 - 数据包	当前会话中接收的数据包的总数。仅限于会话日志。
源端口	TCP 或 UDP 通讯的源端口，对于其他类型的通讯，它将为 “0”。
目的端口	TCP 或 UDP 通讯的目的端口，对于其他类型的通讯，它将为 “0”。
vpn	如果通讯使用了 VPN 通道，则为通讯所使用的通道名。如果通讯不是来自于 VPN 通道，则在日志中没有此项信息。
转换 IP	在 NAT 模式中转换的 IP ；对于透明模式，它将是 “0.0.0.0”。仅限于数据包日志。
转换端口	NAT 模式下转换的端口；对于透明模式，它将是 “0”。仅限于数据包日志。
dir_disp	原始数据包或者应答数据包。仅限于数据包日志。
tran_disp	NAT 转换的源数据包或者 NAT 转换的目的数据包。仅限于数据包日志。

日志消息

本章描述了如下日志消息。

事件日志消息

Admin

危机

分类和 ID: Event-Admin-001

消息:

多次登录失败，用户 < 名称 > 来自 {<ip_ 地址 > | console}。

含义:

该名称的用户三次企图登录失败，可以是来自于一个网络地址或者通过控制端口连接。五次企图登录失败后，Fortinet 设备自动中断连接。

建议行动:

确保管理员使用了正确的登录名和密码。

警告

分类和 ID: Event-Admin-002

消息:

Admin < 管理员 _ 名称 > 已经 { 登录 | 登出 } 通过 { 控制接口 | SSH 来自 <ip_ 地址 > | https 来自 <ip_ 地址 >}。

含义:

该名称的管理员已经通过控制台连接、SSH 会话或者 HTTPS 会话从给定的 IP 地址登录或者登出。

建议行动:

无。

分类和 ID: Event-Admin-003

消息：

管理会话来自 {console | ssh 来自 <ip_ 地址 >| https 来自 <ip_ 地址 >} 对于用户 < 管理员名称 > 已经超时。

含义：

该名称的管理员通过控制台、SSH 或者 HTTPS 建立的管理会话已经过期。

建议行动：

无。

注意

分类和 ID: Event-Conf-001

消息：

< 管理员用户名 > 管理对以下内容的限制 <ip_ 地址 > < 掩码 > 已经 { 添加 | 删除 }。

含义：

管理员可以对能够使用管理员帐户通过网络访问 FortiGate 设备的 IP 地址加以限制，或者去除这一限制。如果去掉了限制，管理员可以从任何 IP 地址管理这个 FortiGate 设备。

建议行动：

确认所做的修改的适当的。

分类和 ID： Event-Conf-002

消息：

< 管理员用户名 > 密码已经修改。

含义：

Admin 用户的密码已经修改。

建议行动：

确认所做的修改的适当的。

分类和 ID： Event-Conf-003

消息：

管理员用户 < 名称 > 已经被 { 添加 | 修改 | 删除 }。

含义：

root 管理员已经添加了该名称的管理员用户，修改了该用户的管理权限，或者删除了该用户。

建议行动：

无。

DHCP

消息

分类和 ID： Event-DHCP-001

消息：

一个 DHCP 分配的 IP 地址 <ip_ 地址 > 已经被 { 分配给 <mac_ 地址 > | 从以下地址释放 <mac_ 地址 >}。

含义：

FortiGate 设备作为一个 DHCP 服务器，已经对给定 MAC 地址的 DHCP 客户分配了 IP 地址，或者从该用户释放了 IP 地址。

建议行动：

无。

分类和 ID： Event-DHCP-002

消息：

MAC 地址 <mac_ 地址 > 检测到一个 IP 冲突并且已经拒绝了地址 <ip_ 地址 >。

含义：

DHCP 客户端已经检测到一个 IP 地址冲突并拒绝了给定的地址。

当分配给 DHCP 客户端一个 IP 地址之后，在这个客户端接受它之前，这个客户端检查是否有其他主机在使用相同的地址。如果这个客户端没有发现冲突，它将接受这个地址。如果它发现存在冲突，它将拒绝这个地址。

建议行动：

无。

注意

分类和 ID： Event-Conf-004

消息：

DHCP 服务器选项已经被修改。

含义：

一个管理员已经修改了一项或多项 DHCP 服务器选项。

建议行动：

无。

系统

警告

分类和 ID： Event-System-001

消息：

系统配置已经被 { 复位 | 下载 | 上载 }。

含义：

一个系统管理员已经将配置文件复位到出厂默认设置或者配置文件已经被上载或下载。

建议行动：

无。

高可用性

危急

分类和 ID： Event-HA-001

消息：

HA 主连接已经变成非活动状态。第二连接变成活动连接。

含义：

主 HA 连接已经关闭并且 HA 现在通过第二连接通讯。

建议行动：

立即恢复 HA 连接。

消息

分类和 ID： Event-HA-002

消息：

HA 状态已经改变为 { 活动 | 非活动 }。

含义：

HA 连接的状态已经从活动改变成非活动，或者从非活动改变成活动。

建议行动：

尽快恢复非活动的 HA 连接。

注意

分类和 ID： Event-Conf-005

消息：

HA 模式已经改变成 { 标准 | 主动 - 主动 | 主动 - 被动 } 由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

该名称的管理员已经修改了 HA 模式。

建议行动：

无。

分类和 ID： Event-Conf-006

消息：

HA 密码已经被用户 <name> 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

该名称的管理员已经修改了 HA 密码。

建议行动：

无。

分类和 ID： Event-Conf-007

消息：

HA 组 ID 已经被修改成 <id> 由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

该名称的管理员已经修改了 HA 组 ID。

建议行动：

无。

分类和 ID： Event-Conf-008

消息：

以下接口正在 HA 状态并被监视： {< 接口名称 >[,]} 由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

该名称的管理员已经将接口修改成 HA 状态并被监视。

建议行动：

无。

系统状态

注意

分类和 ID： Event-System-002

消息：

系统已经从 < 版本号 > 升级到 < 版本号 > 使用固件 < 文件名 > 由管理员 < 管理员名称 > 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

该名称的管理员已经将 FortiGate 固件通过 CLI 或者基于 Web 的管理程序使用该名称的文件升级了。

建议行动：

无。

分类和 ID： Event-System-003

消息：

防病毒定义已经从＜版本号＞升级到＜版本号＞使用定义文件＜文件名＞由管理员＜管理员名称＞ 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

该名称的管理员已经通过 CLI 或者基于 Web 的管理程序使用该名称的文件将病毒定义文件升级到了一个更高的版本。

建议行动：

无。

分类和 ID： Event-System-004

消息：

攻击定义文件已经被从＜版本号＞升级到＜版本号＞ 使用定义文件＜文件名＞由管理员＜管理员名称＞ 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

该名称的管理员已经通过 CLI 或者基于 Web 的管理程序使用该名称的文件将攻击定义文件生计到了一个更高的版本。

建议行动：

无。

分类和 ID： Event-System-005

消息：

系统设置已经备份到如下文件＜文件名＞ 由用户＜用户名＞ 通过 {console | ssh | https | snmp | fortimanager} 完成。

含义：

该名称的用户已经将系统设置备份到了该名称的文件中。

建议行动：

无。

分类和 ID： Event-System-006

消息：

系统设置已经从＜文件名＞中恢复， 由用户＜名称＞ 通过 {console | ssh | https | snmp | fortimanager} 完成。

含义：

该名称的用户使用该文件恢复了系统设置。

建议行动：

无。

分类和 ID： Event-System-007

消息：

系统设置已经被恢复到了出厂状态，由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 完成。

含义：

该名称的用户已经将系统设置恢复到了出厂状态。

建议行动：

无。

分类和 ID： Event-System-008

消息：

运行模式已经被切换到 {NAT | 透明 } 模式， 由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

该名称的用户已经将运行模式切换到了 NAT 或者透明模式。

建议行动：

无。

监视器

注意

分类和 ID： Event-System-009

消息：

会话类型 {tcp | udp} 从 <ip_ 地址 >:< 端口号 > 到 <ip_ 地址 >:< 端口号 > 已经被用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 删除。

含义：

该名称的用户删除了一个 TCP/UDP 会话。

建议行动：

无。

更新

注意

分类和 ID： Event-Conf-009

消息：

更新中心 {1 | 2} 已经被修改为 {<ip_ 地址 > | < 域名 > | none} 由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

该名称的用户已经修改了更新中心 1 或者更新中心 2，修改为无、其他 IP 或者域名。

建议行动：

无。

分类和 ID： Event-Conf-010

消息：

推送中心已经被 { 启用 | 禁用 } ，由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

该名称的用户已经启用或者禁用了推送更新。

建议行动：

无。

分类和 ID： Event-Conf-011

消息：

定期更新已经被 { 禁用 | 启用并修改为 { 每天 < 时 >:< 分 > | 每周 < 日 > < 时 >:< 分 >} } 由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 修改

含义：

该名称的管理员已经禁用了定期更新，或者启用了定期更新并修改了它的设置。

建议行动：

无。

分类和 ID： Event-Conf-012

消息：

病毒定义更新已经被 { 启用 | 禁用 } 由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

该名称的用户以及启用或者禁用了病毒定义更新。

建议行动：

无。

分类和 ID： Event-Conf-013

消息：

攻击定义更新已经被 { 启用 | 禁用 } 由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

该名称的用户已经启用或者禁用了攻击定义更新。

建议行动：

无。

区域

注意

分类和 ID： Event-Conf-014

消息：

区域 <zone_name> 已经被 { 添加 | 修改 | 删除 } 由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

该名称的管理员已经添加、修改或者删除了这个区域。

建议行动：

无。

接口

分类和 ID： Event-Conf-015

消息：

接口 < 名称 > 已经被 { 添加 | 修改 | 删除 | 启用 | 禁用 } 由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

该名称的管理员已经添加、修改、删除、启用或禁用了该名称的接口。

建议行动：

无。

DNS

分类和 ID： Event-Conf-016

消息：

{ 主 | 辅助 } DNS 服务器已经被从 <ip_ 地址 > 修改为 <ip_ 地址 > 由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

改名称的管理员已经修改了主 DNS 服务器或者辅助 DSN 服务器的 IP。

建议行动：

无。

路由表

注意

分类和 ID： Event-Conf-017

消息：

路由 <名称> 已经被 {添加 | 修改 | 删除 } ，由用户 <名称> 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

该名称的管理员已经添加、修改或者删除了给定的路由。

建议行动：

无。

分类和 ID： Event-Conf-018

消息：

RIP 服务器已经被 { 启用 | 禁用 } 由用户 <名称> 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

该名称的管理员已经启用或者禁用了 RIP 服务器。

建议行动：

无。

网关

注意 :

分类和 ID： Event-Conf-019

消息：

一个网关 <ip_ 地址> 已经被 { 添加 | 修改 | 删除 } 由用户 <名称> 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

该名称的管理员已经添加、修改或者删除了指定网关的 IP。

建议行动：

无。

时间

注意

分类和 ID： Event-System-010

消息：

系统时间已经从 NTP 更新。

含义：

系统时间已经通过网络时间协议 （NTP）自动更新。

建议行动：

无。

分类和 ID： Event-Conf-020

消息：

时区已经被修改为 < 时区 _ 名称 > 由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

该名称的管理员已经修改了该系统的时区设置。

建议行动：

无。

分类和 ID： Event-Conf-021

消息：

夏令时的自动时钟调整已经被 { 启用 | 禁用 } 由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

该名称的管理员已经启用或者禁用了夏令时的自动时钟调整选项。

建议行动：

无。

分类和 ID： Event-Conf-022

消息：

系统时间已经被修改成 < 月 >/< 天 >/< 年 >,< 时 >:< 分 >:< 秒 > 由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

该名称的管理员已经修改了系统时间。

建议行动：

无。

分类和 ID： Event-Conf-023

消息：

与 NTP 服务器同步功能已经被 { 启用 | 禁用 } 由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

该名称的管理员已经启用或者禁用了与 NTP 服务器同步时钟的选项。

建议行动：

无。

分类和 ID： Event-Conf-024

消息：

NTP 服务器 IP 地址已经被修改为 <ip_ 地址 > 由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

该名称的管理员已经修改了 NTP 服务器的 IP 地址。

建议行动：

无。

分类和 ID： Event-Conf-025

消息：

NTP 同步时间间隔已经被修改为 < 分钟 > 由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

该名称的管理员已经修改了 NTP 同步时间间隔。

建议行动：

无。

选项

注意

分类和 ID： Event-Conf-026

消息：

空闲超时已经从 < 分钟 > 修改为 < 分钟 > 由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

该名称的管理员已经修改了以分钟为单位的空闲超时时间设置。

建议行动：

无。

分类和 ID： Event-Conf-027

消息：

认证超时已经从 < 分钟 > 修改为 < 分钟 > 由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

该名称的管理员已经修改了认证超时时间设置，这将决定用户认证会话到时的时间设置。

建议行动：

无。

分类和 ID： Event-Conf-028

消息：

语言已经从 < 语言 > 修改为 < 语言 > 由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

该名称的管理员已经修改了系统语言设置。

建议行动：

无。

分类和 ID： Event-Conf-029

消息：

PIN 保护已经被 { 启用 | 禁用 } 由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

该名称的管理员已经启用或者禁用了 PIN 保护功能。

建议行动：

无。

分类和 ID： Event-Conf-030

消息：

PIN 号码已经由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

该名称的管理员已经修改了 PIN 号码。

建议行动：

无。

SNMP

消息

消息：

SNMP 已经从未知团体 < 名称 > 收到一个请求，位于 <ip_ 地址 >:< 端口 >。

含义：

FortiGate 设备已经从特定的 SNMP 管理者收到了一个请求。但是发送请求的团体字符串与 FortiGate 系统的团体字符串不匹配。

建议行动：

如果 SNMP 管理者 IP 地址和端口号是合法的，建议 SNMP 管理者检查团体字符串设置。

注意

分类和 ID： Event-Conf-031

消息：

SNMP 已经被 { 修改 | 启用 | 禁用 } 由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

该名称的管理者已经启用或者禁用 SNMP。

建议行动：

无。

策略

注意

分类和 ID： Event-Conf-032

消息：

Policy 源接口 < 接口 _ 名称 > 目的接口 < 接口 _ 名称 > 编号 <No.> 源地址 < 地址 _ 名称 > 目的地址 < 地址 _ 名称 > 任务计划 < 任务计划 _ 名称 > 服务 < 服务 _ 名称 > 动作 < 动作 _ 名称 > 已经被 { 添加 | 修改 | 删除 | 启用 | 禁用 } 由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

一个管理员已经添加、修改、删除、启用或者禁用了一个访问策略。

建议行动：

无。

地址

注意

分类和 ID： Event-Conf-033

消息：

地址 < 地址 _ 名称 > 已经被 { 添加 | 修改 | 删除 } 由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 完成。

含义：

一个管理员已经添加、修改或者删除了给定的地址。

建议行动：

无。

地址组

注意

分类和 ID： Event-Conf-034

消息：

地址组 < 组 _ 名称 > 已经被 { 添加 | 删除 } 由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 完成。

含义：

一个管理员已经添加或者删除了特定的地址组。

建议行动：

无。

分类和 ID： Event-Conf-035

消息：

地址组 < 组 _ 名称 > 已经被 { 添加 | 删除 } 成员 < 地址名 1> < 地址名 2> ……< 地址名 N> 由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 完成。

含义：

一个管理员已经添加了一个特定地址，或者从该名称的地址组中删除了这个地址。

建议行动：

无。

服务

注意

分类和 ID： Event-Conf-036

消息：

服务 < 服务 _ 名称 > 已经被 { 添加 | 修改 | 删除 } 由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

一个管理员已经添加、修改或者删除了特定的定制服务。

建议行动：

无。

服务组

注意

分类和 ID：Event-Conf-037

消息：

服务组 <组_名称> 已经被 {添加|删除} 由用户 <名称> 通过 {console | ssh | https | snmp | fortimanager} 完成。

含义：

一个管理员已经添加、修改或者删除了特定的服务组。

建议行动：

无。

分类和 ID：Event-Conf-038

消息：

服务组 <组_名称> 已经 {添加|删除} 成员 <服务_名称> 由用户 <名称> 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

一个管理员已经在该名称的服务组中添加或者删除了特定的服务。

建议行动：

无。

任务计划

注意

分类和 ID：Event-Conf-039

消息：

周期性任务计划 <任务计划_名称> 已经被 {添加|修改|删除} 由用户 <名称> 通过 {console | ssh | https | snmp | fortimanager} 完成。

含义：

一个管理员已经添加、修改或者删除了特定的周期性任务计划。

建议行动：

无。

分类和 ID：Event-Conf-040

消息：

一次性任务计划 <任务计划_名称> 已经被 {添加|修改|删除} 由用户 <名称> 通过 {console | ssh | https | snmp | fortimanager} 完成。

含义：

一个管理员已经添加、修改或者删除了特定的一次性任务计划。

建议行动：

无。

虚拟 IP

注意

分类和 ID： Event-Conf-041

消息：

VIP <vip_ 名称 > 外部接口 < 接口 _ 名称 > 外部 IP <ip_ 地址 > 映射到的 IP 已经被 { 添加 | 修改 | 删除 } 由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

一个管理员已经添加、修改或者删除了特定的虚拟 IP。

建议行动：

无。

IP 池

注意

分类和 ID： Event-Conf-042

消息：

IP 池内部接口 < 接口 _ 名称 > 从 <ip_ 地址 > 到 <ip_ 地址 > 已经被 { 添加 | 修改 | 删除 } 由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

一个管理员已经添加、修改或者删除了特定的 IP 池。

建议行动：

无。

IP/MAC 绑定

注意

分类和 ID： Event-Conf-043

消息：

IP/MAC 绑定 <ip_ 地址 > <mac_ 地址 > 已经被 { 添加 | 修改 | 删除 | 启用 | 禁用 } 由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

一个系统管理员已经添加、修改、删除、启用或者禁用静态 IP/MAC 绑定。

建议行动：

无。

分类和 ID： Event-Conf-044

消息：

IPMAC 绑定设置通过防火墙已经被 { 启用 | 禁用 } 由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

一个管理员已经启用或者禁用 IP/MAC 绑定设置。

建议行动：

无。

分类和 ID： Event-Conf-045

消息：

IP/MAC 绑定设置通过防火墙已经被 { 启用 | 禁用 } 由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

一个管理员已经启用或者禁用了 IP/MAC 绑定设置。

建议行动：

无。

分类和 ID： Event-Conf-046

消息：

IP/MAC 绑定设置默认动作已经被 { 允许 | 阻塞 } 由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

一个管理员已经将 IP/MAC 绑定设置默认动作修改为允许或者阻塞。

建议行动：

无。

本地用户

注意

分类和 ID： Event-Conf-047

消息：

本地用户 < 用户名 > 已经被 { 添加 | 修改 | 删除 | 启用 | 禁用 } 由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

一个管理员已经添加、修改、删除、启用或者禁用了特定的本地用户。

建议行动：

无。

RADIUS 服务器

注意

分类和 ID： Event-Conf-048

消息：

RADIUS 服务器 < 服务器名 > 已经被 ｛添加｜修改｜删除｝ 由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

一个管理员已经添加、修改、或者删除了特定的 RADIUS 服务器。

建议行动：

无。

用户组

注意

分类和 ID： Event-Conf-049

消息：

用户组 < 组名 > 已经被 ｛添加｜删除｝ 由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

一个管理员已经添加或者删除了特定的用户组。

建议行动：

无。

分类和 ID： Event-Conf-050

消息：

用户组 < 组名 > 已经 ｛添加｜删除｝ 成员 < 用户名 1 | radius 名称 1>……< 用户名 N | radius 名称 N> 由用户 < 名称 > 通过 {console | ssh | https | snmp | fortimanager} 修改。

含义：

一个管理员已经向该名称的用户组添加了特定的本地用户或者 RADIUS 服务器或者删除了该用户。

建议行动：

无。

病毒日志消息

检测到病毒

消息：

检测到 < 病毒名称 > 病毒，在从 <ip 地址 > 使用 {IMAP | POP3 | SMTP | HTTP} 协议下载的内容中。

含义：

防火墙在下载文件时检测到了一个病毒。

建议行动：

无。

升级了一个特征

消息：

< 特征版本 > 已经被 < 手工 | 自动 | 推送 > 更新。

含义：

病毒数据库已经被更新。

建议行动：

无。

网页过滤日志消息

检测到禁忌词汇

消息：

试图访问包含关键词 < 关键词 > 的网页，IP 地址为 <ip 地址 >。

含义：

从特定 IP 地址的用户试图访问包含被阻塞的关键词的页面。

建议行动：

无。

脚本已经被删除

消息：

试图访问的包含脚本 < 脚本 > 的网页已经被删除，该网页来自 <ip 地址 >。

含义：

脚本已经从网页中删除。

建议行动：

无。

URL 已经被阻塞

消息：

试图访问 <url>，来自 <ip 地址 >。

含义：

来自该地址的用户试图访问阻塞的 URL。

建议行动：

无。

IDS 日志消息

消息：

检测到 < 攻击类型 > 攻击， 来自 <ip 地址 > 。

含义：

检测到来自特定地址的攻击。攻击类型包括以下几种：

001:IP 淹没保护

002:Teardrop 攻击保护

003: 死亡之 Ping 保护

004:IP 源路由过滤保护

005:SYN 淹没保护

006:Land 攻击保护

007:ICMP 淹没保护

008:UDP 淹没保护

009:WinNuke 攻击保护

010: 端口扫描保护

011:IP 交换保护

012:Java/ActiveX/ZIP/EXE 阻塞

013: 通过其他 IPSec 选项

014: 通过 pptp vpn 通讯

015: 通过非 IP 通讯选项

016: 拒绝策略警报

建议行动：

无。



术语表

连接： 两台电脑之间、应用程序之间、进程之间或者其他诸如此类的对象之间的物理上或逻辑上的联系，或者两者都有的联系。

DMZ，非军事区： 用来提供互联网服务而无须允许对内部（私有）网络的未经授权的访问。典型情况下，DMZ 包含了可以访问互联网的服务器，例如网页服务器（HTTP），文件传输服务器（FTP），邮件服务器（SMTP）和域名解析服务器（DNS）。

DMZ 接口： FortiGate 上连接到 DMZ 网络的接口。

DNS，域名解析服务： 把用字母表示的节点名转换为 IP 地址的服务。

以太网：一个局域网（LAN），使用总线型或星型拓扑结构，支持 10Mbps 的传输速率。以太网是被广泛应用的局域网标准之一。新版本的以太网被称做 100 Base-T（或快速以太网），支持 100 Mbps 的数据传输速率。而最新的标准，千兆以太网，支持每秒 1 吉（1,000 兆比特）的数据传输速率。

外部接口： FortiGate 连接到互联网的网络接口。

FTP，文件传输协议： 一个 TCP/IP 协议和应用程序，用于上载或下载文件。

网关： 它包括相应的软件和硬件，用来连接不同的网络。例如，TCP/IP 网络之间的网关可以连接不同的子网。

HTTP，超文本传输协议： 被万维网（WWW）所使用的协议。HTTP 定义了消息的格式和传输方式，以及服务器和浏览器应当如何对不同的命令作出响应。

HTTPS：使用网页浏览器跨过互联网传输私人文件的 SSL 协议。

内部接口： FortiGate 用于连接到内部（私有）网络的网络接口。

互联网： 以 NFSNET 为骨干网，覆盖全球的彼此连接的网络总称。在一般的术语中，也可以表示一些互相连接的网络。

IICMP，互联网控制信息协议：互联网协议（IP）的一部分。它一般被用来发送错误信息、测试数据包以及一些与 IP 有关的信息。当 PING 功能发送 ICMP 响应请求到网络中的一台主机时会用到这一协议。

IKE，互联网密钥交换： 一种在两台安全服务器之间自动交换认证密钥和加密密钥的方法。

IMAP，互联网消息访问协议： 一种互联网电子邮件协议，用来通过任何兼容 IMAP 的浏览器访问您的电子邮件。使用 IMAP 时，您的电子邮件保存在服务器上。

IP，互联网协议： TCP/IP 协议的一部分，处理数据包路由。

IP 地址： 在 TCP/IP 网络中的一台电脑或者设备的识别标志。IP 地址是一个 32 比特的数字地址，通常写成用小数点分隔的四个数字。每个数字都可以是从 0 到 255 中的任何一个。

L2TP，第二层通道协议： 点对点传输协议（PPTP）的扩展，允许互联网服务供应商通过它操作虚拟专用网络（VPN）。L2TP 融合了微软公司的 PPTP 和思科公司的 L2F 系统。要建立一个 L2TP VPN，您的互联网服务供应商的路由器必须支持 L2TP。

IPSec，互联网协议安全： 支持 IP 层上的数据包安全交换的一组协议。IPSec 通常用来支持 VPN。

LAN，局域网：在一个较小范围内建立的网络。大多数局域网连接工作站和个人电脑。局域网上的每个电脑都可以访问位于局域网上任何位置的任何数据和设备。这意味着大多数用户可以把他们的数据象打印机那样的物理资源一样共享。

MAC 地址，介质访问控制地址： 用来唯一识别网络上的每个节点的硬件地址。

MIB，管理信息数据库：可以被简单网络管理协议（SNMP）网络管理程序监控的对象的数据库。

调制解调器： 可以把数字信号转换成模拟信号和把模拟信号转换成数字信号并通过电话线路传输的设备。

MTU，最大传输单元： 一个网络可以传输的数据包的最大物理尺寸，以字节为单位。任何大于 MTU 的数据包在发送之前都会被分成较小的数据包。理想情况下，网络中的 MTU 应当等于从您的电脑到目的地之间所经过的所有网络中的最小 MTU。如果您的消息大于其中的任何一个 MTU，它们会把它分割 （破碎），这将会减慢传输速度。

网络掩码： 也称做子网掩码。忽略了一个完整的 IP 地址中的一部分的一组规则，从而可以无须广播就可以达到目的地址。它表示一个大的 TCP/IP 网络中的子网部分。有时用来表示一个地址掩码。

NTP，网络时间协议： 用来把一台电脑的时间同步为 NTP 服务器的时间。NTP 互联网提供精确到十毫秒以内的互联网时间 （UTC）。

包： 通过包交换网络传送的消息的一部分。包的一个关键特征是它除了数据之外还包含了目的地的地址。在 IP 网络中包通常被称做数据包。

Ping，数据包互联网分组： 一个用来判定特定 IP 地址是否可以访问的工具。它的工作原理是向指定的地址发送一个数据包并等待回复。

POP3，邮局协议： 用于从邮件服务器通过互联网向邮件客户端传输电子邮件的协议。多数电子邮件客户端使用 POP 协议。

PPP, 点对点传输协议： 提供了主机到网络和路由器到路由器的连接的 TCP/IP 协议。

PPTP，点对点通道协议： 基于 Windows 的建立虚拟专用网络的技术。Windows98，Windows2000 和 WindowsXP 都支持 PPTP 协议。要建立 PPTP 虚拟专用网络，您的 ISP 的路由器必须支持 PPTP。

端口： 在 TCP/IP 和 UDP 网络中，端口是逻辑连接的终点。端口号标识了端口的类型。例如，80 端口用于 HTTP 协议的数据传输。

协议：两个设备之间商定的传输数据的格式。协议决定了要使用的错误检测的类型，数据压缩的方法 （如果有的话），发送设备如何指示它完成了一个消息的发送，接收设备如何指示它已经完成了一个消息的接收。

RADIUS, 远程拨号访问用户认证服务： 很多 INTERNET 服务供应商 （ISP）使用的认证和计帐系统。当用户拨入一个 ISP 时，他们输入一个用户名和密码。这些信息被传送到 RADIUS 服务器，RADIUS 检验这些信息的正确性，然后授予访问 ISP 系统的权限。

路由器： 把局域往连接到互联网并为他们之间的数据提供路由的设备。

路由： 决定发送数据到目的地时要经过的路径的过程。

路由表：含有一系列有效的数据传送路径的列表。

服务： 应答其他设备 （客户）的请求的应用程序。通常用来描述任何在网络上提供类似打印、海量存储、网络访问等服务的设备。

SMTP，简单邮件传输协议：在 TCP/IP 网络中提供邮件发送服务的程序。

SNMP，简单网络管理协议： 一组网络管理协议。SNMP 对网络的不同部分发送消息。支持 SNMP 的设备，称做代理，把他们自己的数据存储在管理信息库 （MIB） 中，并且把这些信息返回给 SNMP 请求的发送者。

SSH，安全命令解释器： 远程登录程序安全的替代品。您可以用它跨过网络登录到其他电脑上并执行命令。SSH 通过安全通道提供了强大的安全认证和安全通信。

子网： 网络具有相同子网地址的部分。在 TCP/IP 网络中，子网定义为所有 IP 地址前缀相同的设备。例如，所有 IP 地址从 100.100.100 开始的设备属于同一子网。从安全和性能角度考虑，把网络分割成子网是必要的。IP 网络使用子网掩码分割子网。

子网地址： IP 地址中标识子网的部分。

TCP，传输控制协议： TCP/IP 网络的主要部分之一。TCP 保证了数据的提交，也保证了数据包能够按照它们被发送时的顺序提交。

UDP，用户数据报协议：一种无连接协议。类似于 TCP，运行于 IP 网络的顶端。与 TCP 协议不同的是，UDP 提供很少的纠错服务，取而代之的是提供了通过 IP 网络发送和接收数据报的直接传输途径。它主要用于在网络上广播消息。

VPN，虚拟专用网： 一个跨越在 INTERNET 上类似于私有网络的网络。VPN 使用加密和其它安全机制来保证只有经过认证的用户可以访问网络，并且数据不会被篡改。

病毒：一种把自己附加到别的程序上的电脑程序，并通过这种机制在电脑中或网络上传播，通常具有有害的企图。

蠕虫：通过电脑网络复制自己的程序或算法，通常使用电子邮件，并且会进行一些恶意的活动，例如耗尽电脑系统的资源并且可能导致系统关闭。



索引

J

K

L

M

N

P

R

S

T

V

W

X

Y

Z